3GPP TSG-SA WG3 (Security)

Report to SA Meeting # 4,

Miami, USA

21-23 June 1999

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Summary of documents tabled by SA3
- Status of deliverables - followed by approval of specifications/report
- Summary of security priorities
- Status of algorithm design
- Equipment security - decision on way forward
- VHE security

Document List,1

- SP-99nnn Report of SA WG3 meeting, 11-12 May, Bonn - *for information*
- SP-99nnn Draft Report of SA WG3 meeting, 16-18 June, London - *for information*
- SP-99284 Status of SA WG3 deliverables & priorities - *for information & discussion*
- SP-99nnn Criteria for cryptographic algorithm design process - *Technical Report for approval*

Document List,2

- SP-99nnn Integration requirements - *Draft technical specification for information*
- SP-99nnn Cryptographic algorithm requirements - *Technical specification for approval*
- SP-99nnn Lawful interception requirements - *Technical specification for approval*
- SP-99nnn CRs to Security architecture - *CRs to technical specification (3G TS 33.102) for approval*

Status of 3GPP Security Deliverables, 1

3GPP security specification	Rapporteur	Milestones	Status
Objectives and principles	Tim Wright		1st release approved by SA # 2
Threats and requirements	Per Christofferson		1st release approved by SA # 3
Architecture	Bart Vinck and Stefan Puetz		1st release approved by SA # 3

Status of 3GPP Security Deliverables, 2

3GPP security specification	Rapporteur	Milestones	Status
Integration requirements	Colin Blanchard	**Draft for information to SA #4**	May release delayed to July
Cryptographic algorithm requirements	Takeshi Chikawaza	**For approval at SA #4**	1st release approved SA3
Criteria for cryptographic algorithm design process	Gert Roelofsen/Rolf Blom	**For approval at SA #4** (Method approved SA #3)	1st release approved SA3

vodafone

Status of 3GPP Security Deliverables, 3

3GPP security specification	Rapporteur	Milestones	Status
Lawful interception requirements	Berthold Wilhelm	**For approval at SA # 4**	1st release approved by SA 3 (work joint with SMG10 WPD)
Lawful interception architecture and functions	Berthold Wilhelm	Scope by end of June	
Guide to 3G security	Charles Brookson	Scope by end of June	

Status of 3GPP Security Deliverables, 4

- CRs to architecture covering following:
  - data integrity of signalling
  - location of ciphering
  - use of authentication data
  - re-synchronisation for AKA
  - sequence number management
  - criteria for replacing authentication
  - network domain security
  - cipher key lifetime

Status of 3GPP Security Deliverables, 5

- CRs to architecture (continued):
  - user bdomain security
  - replacement of incorrect diagrams
  - status of annex B
- New milestones leading to final versions of deliverables to be agreed with editors in July
- *Approval of documents*

Priorities of work items, 1
SP-99284

- Ciphering mechanism
  - Essential for R99
- Integrity protection mechanism
  - Essential for R99
- Authentication and key agreement mechanism
  - Essential for R99

Priorities of work items, 2

- Network wide encryption mechanism
  - Appropriate hooks must be provided in R99
- User identity confidentiality
  - Specification of transport mechanism for enhanced confidentiality mechanism essential for R99
- Core network signalling security
  - Although high priority, recognise that integration into signalling specifications may not be achievable in R99

Priorities of work items, 3

- GSM/UMTS intersystem operation
  - Driven by service requirement. Currently believed to be feasible to specify secure procedures in R99.
- Lawful interception architecture
  - Essential for R99. Can be largely based on GSM/GPRS
- USIM application security
  - Essential for R99. Can just refer to GSM SATK. Enhancements considered in later releases

Priorities of work items, 4

- Fraud information gathering system
  - Essential for R99. Can just refer to GSM FIGS. Enhancements considered in later releases
- Visibility and configurability
  - Encryption indicator essential for R99
- Mobile Execution Environment
  - Essential for R99. Can just refer to GSM MExE. Enhancements considered in later releases

Priorities of work items, 5

- Location services
  - Essential for R99 if location services specified for R99. Priority is unclear.
- IP security
  - Priority is unclear. Impact of IP technologies such as Mobile IP not fully understood.
- Terminal security
  - Requirement is unclear - see later slide

Status of Algorithm Design

- Process for algorithm design approved at SA # 3 (see next slide)
- 3G PCG informed of process by letter 24 May, and funding (Euro 350,000) requested
- Concern with process - paper by MW to go to PCG meeting on 6/7 July, should put minds at rest
- SAGE able to start work in principle in July - candidate algorithms already under consideration

Status of Algorithm Specification

- SA3 agreed position for acquiring algorithms:
  - SA3 to generate algorithm requirements
  - Requirements to algorithm design group (e.g. ETSI SAGE)
  - Design or select algorithm, internal evaluation and commission a closed external expert evaluation
  - Publish design for public evaluation - possibly running in parallel with implementation phase
- Process for responding to public criticism needed

Terminal Security, 1

- It is possible to provide on-air terminal based security features (eg real-time barring of stolen phones, charging dependent on terminal type)
- But these require a secure terminal identification procedure which can be executed on the air:
    - secure storage in the terminal of its identity and secret security associated data
    - a reliable and secure over-the-air protocol to verify the identity of the terminal

Terminal Security, 2

- Secure storage must prevent unauthorised change of the terminal identity and unauthorised reading of secret data - the method does not need to be standardised
- Secure over-the-air identification protocols that do not require a network to *own* the terminal can be based on public key cryptography (zero knowledge or digital signatures) - a method would need to be standardised

Terminal Security, 3

- The solution will not come for nothing:
  - the identity and associated secret parameters in the terminal will need a level of protection equivalent to that afforded the IMSI and Ki in the GSM SIM
  - the protocol for verifying the terminal identity will be more complex and bandwidth hungry than user authentication - because of public key techniques

Terminal Security, 4

- Will manufactures be any better at securing 3G terminal identities than they have been with GSM?
- Should we go a head and standardise a protocol?
- Any such protocol will be a waste of time if manufacturers fail to secure terminal identities - just like EIR checking in GSM is pointless
- If we do not go ahead, we have to acknowledge that terminal off-air identities can not be relied upon

VHE Security

- Meeting to be held at this meeting to determine requirements for VHE security

Meeting Schedule

May	*11-12*	*Bonn*
June	*17-18*	*London*
August	3-6	Sophia Antipolis (with SMG10)
August	24	Bonn (joint T3 & SA2?)
October	26-27	The Hague
November	16-19	TBD (with SMG10)
December	7-8	Helsinki